

English Translation of Relevant Portions of JP-A-H11-298470
Published on October 29, 1999

:

:

Page (4), column 6, line 39 – Page (5), column 7, line 8

[0006] According to the present invention, a key manager divides a secret key S into a plurality of pieces of secret data S1 to Sn, loads at least one of the divided pieces of secret data Si on a storage medium (including one having a calculation function such as an IC card), and delivers the storage medium to a key user off-line. As to the rest of the divided pieces of secret data, they are sent to said key user on-line only when said key user is authenticated based on authentication data AS generated based on the secret data Si and identification data ID given to said key user.

[0007] In this way, even if the storage medium distributed off-line is stolen by an unauthorized person, it does not mean that the unauthorized person has obtained all the pieces of secret data S1 to Sn that are indispensable to decrypt the secret key S. Likewise, even if the secret data sent on-line is stolen by an unauthorized person, it does not mean that the unauthorized person has obtained all the pieces of secret data S1 to Sn that are indispensable to decrypt the secret key S. This makes it possible to reduce the possibility of secret key data being stolen while it is being distributed, and thus to improve the security of encrypted communication.

:

:

Page (7), column 11, lines 27-32

[0050] When the key user is authenticated by the above described authentication process, the encrypting/decrypting section 103 in the key manager device 100 encrypts the secret data S2 using the secret data S1 as a key. The communication section 107 in the key manager device 100 sends the encrypted secret data S2 to the key user device 200 via the communication line 400.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-298470

(43)Date of publication of application : 29.10.1999

(51)Int.Cl.

H04L 9/08

H04L 9/10

H04L 9/32

(21)Application number : 10-106437

(71)Applicant : HITACHI LTD

(22)Date of filing : 16.04.1998

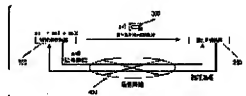
(72)Inventor : YAMAZAKI MASANORI
NISHIOKA GENJI

(54) KEY DISTRIBUTION METHOD AND SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To reduce the possibility of being arrogated by an illegal person when distributing the secret key information to key users.

SOLUTION: A key manager device 100 divides a secret key S into secret information sets S1, S2, stores the information S1 to a storage medium 300 and distributes the information S1 to key users in off-line. A key user device 200 uses the secret information S1 having been stored in a distributed storage medium and identification information ID provided in advance for key users to make authentication processing with the key manager device 100. When the key user device 200 is authenticated, the key manager device 100 sends the remaining secret information S2 through a communication line 400 in on-line. The key user device 200 decodes the secret key S1 based on the secret information distributed in off-line and the secret key S2 sent in on-line.



特開平11-298470

(43) 公開日 平成11年(1999)10月29日

| (51) Int.Cl.* | 識別記号 | F I |
|------------------------------|------|----------------------|
| H 0 4 L 9/08 | | H 0 4 L 9/00 6 0 1 E |
| 9/10 | | 6 0 1 B |
| 9/32 | | 6 0 1 A |
| | | 6 2 1 A |
| | | 6 7 5 D |
| 審査請求 未請求 請求項の数14 O L (全 9 頁) | | |

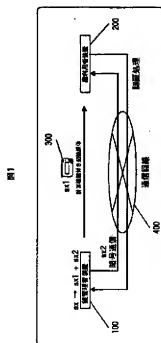
| | | | |
|-----------|------------------|----------|--|
| (21) 出願番号 | 特願平10-106437 | (71) 出願人 | 000005108 株式会社日立製作所 東京都千代田区神田駿河台四丁目6番地 |
| (22) 出願日 | 平成10年(1998)4月16日 | (72) 発明者 | 山▲崎▼ 正重 神奈川県川崎市麻生区王禅寺1099番地 株 式会社日立製作所システム開発研究所内 |
| | | (72) 発明者 | 西岡 玄次 神奈川県川崎市麻生区王禅寺1099番地 株 式会社日立製作所システム開発研究所内 |
| | | (74) 代理人 | 弁理士 富田 和子 |

(54) 【発明の名称】 鍵の配布方法およびシステム

(57) 【要約】

【課題】鍵管理者が鍵利用者に秘密鍵情報を配布する際、当該秘密鍵情報が不正者に横取りされる可能性を減少させる。

【解決手段】鍵管理者装置100は、秘密鍵Sを秘密情報S1、S2に分割し、S1を記憶媒体300に格納して鍵利用者にオフラインで配布する。鍵利用者装置200は、配布された記憶媒体に格納されている秘密情報S1と予め鍵利用者に付与された識別情報IDとを用いて、鍵管理者装置100との間で認証処理を行う。認証された場合、鍵管理者装置100は、残りの秘密情報S2を、通信回線400を介して、オンライン送信する。鍵利用者装置200は、オフライン配布された秘密情報S1とオンライン送信された秘密情報S2とを基に秘密鍵Sを復元する。



【特許請求の範囲】

【請求項1】 暗号通信に用いる鍵の配布方法であって、鍵管理者の装置において、

秘密鍵Sを作成し、当該秘密鍵Sを少なくとも2つの秘密情報S1～Sn ($n \geq 2$) に分割する第1のステップと、

前記第1のステップで得た秘密情報S1～Snのうちの少なくとも1つの秘密情報Si ($1 \leq i \leq n$) をオフラインで鍵利用者に配布する第2のステップと、

鍵利用者の装置において、

前記第2のステップによりオフラインで配布された秘密情報Siと、鍵管理者により予め付与された識別情報IDとを基に、認証情報ASを作成し、当該認証情報ASを鍵管理者の装置に送信する第3のステップと、

鍵管理者の装置において、

前記第3のステップにより送信された認証情報ASに基づいて、鍵利用者の認証処理を行う第4のステップと、前記第4のステップにて鍵利用者が認証された場合、当該鍵利用者の装置に、前記第1のステップで得た秘密情報S1～Snのうち、前記第2のステップで当該鍵利用者にオフラインで配布した秘密情報Si以外の秘密情報を送信する第5のステップと、

鍵利用者の装置において、

前記第5のステップにより送信された、秘密情報Si以外の秘密情報S1～Snと、前記第2のステップによりオフラインで配布された秘密情報Siとを基に、前記秘密鍵Sを作成する第6のステップと、を備えることを特徴とする鍵の配布方法。

【請求項2】 請求項1記載の鍵の配布方法であって、

前記第5のステップは、前記第4のステップにて鍵利用者が認証された場合、当該鍵利用者の装置に、前記第1のステップで得た秘密情報S1～Snのうち、前記第2のステップで当該鍵利用者にオフラインで配布した秘密情報Si以外の秘密情報を、前記秘密情報Siを鍵として暗号化して送信するものあり、

前記第6のステップは、前記第5のステップにより送信された、秘密情報Si以外の暗号化された秘密情報S1～Snを、前記秘密情報Siを鍵として復号化し、復号結果と前記秘密情報Siとを基に、前記秘密鍵Sを作成するものであることを特徴とする鍵の配布方法。

【請求項3】 請求項1または2記載の鍵の配布方法であって、

鍵利用者の装置において、

前記第6のステップにより復元された秘密鍵Sを基に、認証情報AS'を作成し、当該認証情報AS'を鍵管理者の装置に送信する第7のステップと、

鍵管理者の装置において、

前記第7のステップにより送信された認証情報AS'に基づいて、鍵利用者の認証処理を行う第8のステップと、

鍵管理者の装置および/または鍵利用者の装置において前記第8のステップにて鍵利用者が認証された場合に、当該鍵利用者の、前記秘密鍵Sを用いた暗号通信に対する登録料金の課金処理を行う第9のステップを、さらに備えることを特徴とする鍵の配布方法。

【請求項4】 鍵を生成する鍵管理者装置と、当該鍵管理者装置が生成した鍵を用いて暗号通信を行う鍵利用者装置と、となる鍵の配布システムであって、

前記鍵管理者装置は、

10 秘密鍵Sを作成し、当該秘密鍵Sを少なくとも2つの秘密情報S1～Sn ($n \geq 2$) に分割する鍵生成手段と、前記鍵生成手段で得た秘密情報S1～Snのうちの少なくとも1つの秘密情報Si ($1 \leq i \leq n$) を記憶媒体に記憶する記憶手段と、

前記鍵利用者装置から送信された認証情報ASを受信する第1の受信手段と、

前記受信手段で受信した認証情報ASに基づいて、鍵利用者の認証処理を行う認証手段と、

前記認証手段により鍵利用者が認証された場合、前記鍵利用者装置に、前記鍵生成手段で得た秘密情報S1～Snのうち、前記記憶手段で記憶媒体に記憶した秘密情報Si以外の秘密情報を送信する第1の送信手段と、を備え、

前記鍵利用者装置は、

前記鍵管理者装置により秘密情報Siが記憶された記憶媒体から、前記秘密情報Siを読み出す読出手段と、

前記読出手段により読み出された秘密情報Siと、鍵管理者により予め付与された識別情報IDとを基に、認証情報ASを作成する認証情報作成手段と、

30 前記認証情報作成手段により作成された認証情報ASを前記鍵管理者装置に送信する第2の送信手段と、

前記鍵管理者装置により送信された、秘密情報Si以外の秘密情報S1～Snを受信する第2の受信手段と、

前記読出手段により読み出された秘密情報Siと、前記第2の受信手段で受信した、秘密情報Si以外の秘密情報S1～Snとを基に、前記鍵管理者装置が生成した秘密鍵Sを復元する鍵復元手段と、を備えることを特徴とする鍵の配布システム。

【請求項5】 鍵を生成する鍵管理者装置と、当該鍵管理者装置が生成した鍵を用いて暗号通信を行う鍵利用者装置と、計算機能付き記憶媒体と、となる鍵の配布システムであって、

前記鍵管理者装置は、

秘密鍵Sを作成し、当該秘密鍵Sを少なくとも2つの秘密情報S1～Sn ($n \geq 2$) に分割する鍵生成手段と、前記鍵生成手段で得た秘密情報S1～Snのうちの少なくとも1つの秘密情報Si ($1 \leq i \leq n$) を、前記計算機能付き記憶媒体に記憶する記憶手段と、

40 前記鍵利用者装置から送信された認証情報ASを受信する第1の受信手段と、

前記受信手段で受信した認証情報 A S に基づいて、鍵利用者の認証処理を行う認証手段と、

前記認証手段により鍵利用者が認証された場合、前記鍵利用装置に、前記鍵生成手段で得た秘密情報 S 1 ~ S n のうち、前記記憶手段で前記計算機能付き記憶媒体に記憶した秘密情報 S i 以外の秘密情報を送信する第 1 の送信手段と、を備え、

前記鍵利用装置は、

前記計算機能付き記憶媒体を接続する接続手段と、

前記接続手段により接続された前記計算機能付き記憶媒体から出力された認証情報 A S を前記鍵管理者装置に送信する第 2 の送信手段と、

前記鍵管理者装置から送信された、秘密情報 S i 以外の秘密情報 S 1 ~ S n を受信して、前記接続手段により接続された前記計算機能付き記憶媒体に出力する第 2 の受信手段と、を備え、

前記計算機能付き記憶媒体は、

記憶している秘密情報 S i と鍵管理者により予め付与された識別情報 I D とをを、認証情報 A S を作成し、自己が接続している前記鍵利用装置に出力する認証情報作成手段と、

記憶している秘密情報 S i と、自己が接続している前記鍵利用装置から出力された、秘密情報 S i 以外の秘密情報 S 1 ~ S n とを、前記鍵管理者装置で生成した秘密鍵 S を復元する鍵復元手段と、を備えることを特徴とする鍵の配布システム。

【請求項 6】 暗号通信を行う鍵利用者に鍵を配布する情報処理装置であって、

秘密鍵 S を作成し、当該秘密鍵 S を少なくとも 2 つの秘密情報 S 1 ~ S n ($n \geq 2$) に分割する鍵生成手段と、前記鍵生成手段で得た秘密情報 S 1 ~ S n のうちの少なくとも 1 つの秘密情報 S i ($1 \leq i \leq n$) を記憶媒体に記憶する記憶手段と、

鍵利用者の装置から送信された、秘密情報 S i と当該鍵利用者に予め付与した識別情報とを基に作成された認証情報 A S を受信する受信手段と、

前記受信手段で受信した認証情報 A S に基づいて、鍵利用者の認証処理を行う認証手段と、

前記認証手段により鍵利用者が認証された場合、当該鍵利用者の装置に、前記鍵生成手段で得た秘密情報 S 1 ~ S n のうち、前記記憶手段で記憶媒体に記憶した秘密情報 S i 以外の秘密情報を送信する送信手段と、を備えることを特徴とする情報処理装置。

【請求項 7】 請求項 6 記載の情報処理装置であって、前記認証手段により鍵利用者が認証された場合、前記鍵生成手段で得た秘密情報 S 1 ~ S n のうち、前記記憶手段で記憶媒体に記憶した秘密情報 S i 以外の秘密情報を、前記秘密情報 S i を鍵として暗号化し、前記送信手段に出力する暗号化手段をさらに備えることを特徴とする情報処理装置。

【請求項 8】 請求項 6 または 7 記載の情報処理装置であって、

前記受信手段は、鍵利用者の装置から送信された、秘密鍵 S を基に作成された認証情報 A S を受信するものであり、

前記認証手段は、前記受信手段で受信した認証情報 A S に基づいて、鍵利用者の認証処理を行うものであり、前記認証手段により、認証情報 A S に基づいて鍵利用者が認証された場合に、当該鍵利用者の、前記秘密鍵 S を用いた暗号通信に対する登録料金を特定する情報を記憶する課金手段を、さらに備えることを特徴とする情報処理装置。

【請求項 9】 鍵管理者の装置にて、秘密鍵 S を少なくとも 2 つに分割することで得られた秘密情報 S 1 ~ S n ($n \geq 2$) を基に鍵を復元する情報処理装置であって、鍵管理者から配布された記憶媒体に記憶された秘密情報 S i ($1 \leq i \leq n$) を読み出す読出手段と、

前記読出手段により読み出された秘密情報 S i と、鍵管理者により予め付与された識別情報 I D とを、認証情報 A S を作成する認証情報作成手段と、

前記認証情報作成手段により作成された認証情報 A S を鍵管理者の装置に送信する送信手段と、

鍵管理者の装置から送信された、秘密情報 S i 以外の秘密情報 S 1 ~ S n を受信する受信手段と、前記読出手段により読み出された秘密情報 S i と、前記受信手段で受信した、秘密情報 S i 以外の秘密情報 S 1 ~ S n とを、秘密鍵 S を復元する鍵復元手段と、を備えることを特徴とする情報処理装置。

【請求項 10】 請求項 9 記載の情報処理装置であって、鍵管理者の装置から送信された、秘密情報 S i 以外の秘密情報 S 1 ~ S n は、秘密情報 S i を鍵として暗号化されたものであり、

前記受信手段で受信した、秘密情報 S i 以外の暗号化された秘密情報 S 1 ~ S n を、前記読出手段により読み出された秘密情報 S i を鍵として復号化し、前記鍵復元手段に出力する復号化手段をさらに備えることを特徴とする情報処理装置。

【請求項 11】 請求項 9 または 10 記載の情報処理装置であって、

前記認証情報作成手段は、前記鍵復元手段により復元された秘密鍵 S を基に、認証情報 A S を作成するものであり、

前記送信手段は、前記認証情報作成手段により作成された認証情報 A S を鍵管理者の装置に送信するものであり、

鍵管理者の装置にて、前記認証情報 A S により鍵利用者が認証された場合に、当該鍵利用者の、前記秘密鍵 S を用いた暗号通信に対する登録料金を特定する情報を記憶する課金手段を、さらに備えることを特徴とする情報処理装置。

【請求項12】鍵管理者の装置にて、秘密鍵Sを少なくとも2つに分割することで得られた秘密情報S1～Sn ($n \geq 2$)を基に鍵を復元する、当該鍵を用いて暗号通信を行う鍵利用者の装置に挿入可能に構成された計算機能付き記憶媒体であって、

記憶している秘密情報Si ($1 \leq i \leq n$)と、鍵管理者により予め付与された識別情報IDとを基に認証情報ASを作成し、自己が接続している鍵利用者の装置を介して、鍵管理者の装置に送信する認証情報作成手段と、鍵管理者の装置により記憶された秘密情報Siと、自己が接続している鍵利用者の装置を介して受け取った、鍵管理者の装置が送信した秘密情報Si以外の秘密情報S1～Snとを基に、前記秘密鍵Sを復元する鍵復元手段と、を備えることを特徴とする計算機能付き記憶媒体。【請求項13】請求項12記載の計算機能付き記憶媒体であって、

鍵管理者の装置から送信された、秘密情報Si以外の秘密情報S1～Snは、秘密情報Siを鍵として暗号化されたものであり、自己が接続している前記鍵利用者装置が受信した、秘密情報Si以外の暗号化された秘密情報S1～Snを、記憶している秘密情報Siを鍵として復号化し、前記鍵復元手段に出力する復号化手段をさらに備えることを特徴とする計算機能付き記憶媒体。

【請求項14】請求項12または13記載の計算機能付き記憶媒体であって、前記認証情報作成手段は、前記鍵復元手段により復元された秘密鍵Sを基に、認証情報ASを作成し、自己が接続している鍵利用者の装置を介して、鍵管理者の装置に送信するものであり、

鍵管理者の装置にて、前記認証情報ASにより鍵利用者が認証された場合に、当該鍵利用者の、前記秘密鍵Sを用いた暗号通信に対する暗号料金を特定する情報を記憶する課金手段を、さらに備えることを特徴とする計算機能付き記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する分野】本発明は、暗号通信に用いる鍵を鍵利用者(たとえば、暗号データの受信者)に配布する技術に関する。

【0002】

【従来の技術】一般に、大量のデータを暗号通信する場合、秘密鍵暗号が用いられている。秘密鍵暗号では、送信者と受信者との間で共通の鍵(共通鍵)を持つ必要がある。共通鍵の配送方法としては、コピー機方式、個別鍵方式等があるが、いずれの場合においても、秘密鍵情報を受信者に配布しなければならない。従来は、たとえば、ICカード等に秘密鍵情報を搭載して、受信者にオンラインで配布したり、あるいは、暗号通信等により受信者に秘密鍵情報を送信することで、秘密鍵情報を受信

者に配布している。

【0003】

【発明が解決しようとする課題】しかしながら、秘密鍵情報をICカード等に搭載してオフラインで配布する方法では、不正者がこの記憶媒体を盗用し、正規の受信者になります可能性が考えられる。また、秘密鍵情報を暗号通信等により送信する方法では、不正者が秘密鍵情報を盗聴・解読し、正規の受信者になります可能性が考えられる。

【0004】本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、秘密鍵情報を配布する際に、当該秘密鍵情報が不正者に横取りされる可能性を減少させ、暗号通信のセキュリティを向上させることにある。

【0005】

【課題を解決するための手段】上記課題を解決するために、本発明は、暗号通信に用いる鍵の配布方法であって、鍵管理者の装置において、秘密鍵Sを作成し、当該秘密鍵Sを少なくとも2つの秘密情報S1～Sn ($n \geq 2$)に分割する第1のステップと、前記第1のステップで得た秘密情報S1～Snのうちの少なくとも1つの秘密情報Si ($1 \leq i \leq n$)をオンラインで鍵利用者に配布する第2のステップと、鍵利用者の装置において、前記第2のステップによりオフラインで配布された秘密情報Siと、鍵管理者により予め付与された識別情報IDとを基に、認証情報ASを作成し、当該認証情報ASを鍵管理者の装置に送信する第3のステップと、鍵管理者の装置において、前記第3のステップにより送信された認証情報ASに基づいて、鍵利用者の認証処理を行う第4のステップと、前記第4のステップにて鍵利用者が認証された場合、当該鍵利用者の装置に、前記第1のステップで得た秘密情報S1～Snのうち、前記第2のステップで当該鍵利用者にオフラインで配布した秘密情報Si以外の秘密情報を送信する第5のステップと、鍵利用者の装置において、前記第5のステップにより送信された、秘密情報Si以外の秘密情報S1～Snと、前記第2のステップによりオフラインで配布された秘密情報Siとを基に、前記秘密鍵Sを作成する第6のステップと、を備えることを特徴とする。

【0006】本発明によれば、鍵管理者は、秘密鍵Sを複数の秘密情報S1～Snに分割し、そのうちの少なくとも1つの秘密情報Siを記憶媒体(ICカード等の計算機能付き記憶媒体を含む)に搭載してオフラインで鍵利用者に配布している。そして、残りについては、秘密情報Siおよび鍵利用者に付与された識別情報IDを基に作成した認証情報ASにより鍵利用者を認証した場合にのみ、当該鍵利用者にオンラインで送信するようにしている。

【0007】このようにすることで、たとえば、オフラインで配布した記憶媒体が不正者に盗用されたとしても、それだけでは、不正者は、秘密鍵Sを復元するのに必要

なすすべての秘密情報S1～Snを取得したことになる。同様に、オンラインで送信した秘密情報が不正者に盗聴されたとしても、それだけでは、不正者は、秘密鍵Sを復元するのに必要なすべての秘密情報S1～Snを取得したことになる。このため、秘密鍵情報を配布する際に、当該秘密鍵情報が不正者に横取りされる可能性を減少させることができ、ひいては、暗号通信のセキュリティを向上させることができる。

【0008】なお、本発明において、第5のステップは、第4のステップにて鍵利用者が認証された場合、当該鍵利用者の装置に、前記第1のステップで得た秘密情報S1～Snのうち、前記第2のステップで当該鍵利用者にオフラインで配布した秘密情報Si以外の秘密情報、前記秘密情報Siを鍵として暗号化して送信するものであり、第6のステップは、第5のステップにより送信された、秘密情報Si以外の暗号化された秘密情報S1～Snを、前記秘密情報Siを鍵として復号化し、復号結果と前記秘密情報Siとを基に、前記秘密鍵Sを作成するものでもよい。

【0009】このようにすることで、秘密情報Si以外の秘密情報S1～Snをオンラインで送信する際のセキュリティをさらに向上させることができる。

【0010】

【発明の実施の形態】以下に、本発明の一実施形態について説明する。

【0011】図1は、本発明の一実施形態である秘密鍵配布方法が適用されたシステムの概略図である。

【0012】図示するように、本実施形態方法は、相互に通信回線400で接続された鍵管理者装置100および鍵利用者装置200と、鍵管理者装置100および鍵利用者装置200に挿抜可能に構成された計算機能付き記憶媒体300と、を含んで構成されるシステムにおいて実施される。

【0013】図2に、鍵管理者装置100の概略機能構成を示す。

【0014】図示するように、鍵管理者装置100は、乱数生成部101と、演算部102と、暗復号化部103と、認証部104と、鍵金部105と、メモリ106と、通信部107と、で構成される。これらの機能構成は、コンピュータにおいて、各機能を実現するための手順が記述されたプログラムを実行することにより、ソフトウェア的に実現されるものでもよいし、あるいは、各機能を実現するロジックを組むことによりハードウェア的に実現されるようにしてもよい。ソフトウェア的に実現される場合は、各機能を実現するための手順が記述されたプログラムを、CD-ROM等の記憶媒体に格納して、コンピュータに供給するようにしてもよい。

【0015】なお、鍵管理者装置100は、オフラインで鍵利用者装置200に配布する計算機能付き記憶媒体300を接続するための機構が設けられている。

【0016】図3に、鍵利用者装置200の概略機能構成を示す。

【0017】図示するように、鍵利用者装置200は、乱数生成部201と、素数生成部202と、演算部203と、暗復号化部204と、メモリ205と、通信部206と、で構成される。これらの機能構成は、鍵管理者装置100と同様、コンピュータにおいて、各機能を実現するため手順が記述されたプログラムを実行することにより、ソフトウェア的に実現されるものでもよいし、あるいは、各機能を実現するロジックを組むことによりハードウェア的に実現されるようにしてもよい。ソフトウェア的に実現される場合は、各機能を実現するための手順が記述されたプログラムを、CD-ROM等の記憶媒体に格納して、コンピュータに供給するようにしてもよい。

【0018】なお、鍵利用者装置200は、オフラインで鍵管理者から配布された計算機能付き記憶媒体300を接続するための機構が設けられている。

【0019】図4に、計算機能付き記憶媒体300の概略機能構成を示す。

【0020】図示するように、計算機能付き記憶媒体300は、暗復号化部301と、演算部302と、メモリ303と、で構成される。これらの機能構成は、ICカードにおいて、各機能を実現するため手順が記述されたプログラムを実行することにより、ソフトウェア的に実現されるものでもよいし、あるいは、各機能を実現するロジックを組むことによりハードウェア的に実現されるようにしてもよい。

【0021】次に、上記説明したシステムにおいて実施される、本発明の第一実施形態である秘密鍵配布方法について説明する。

【0022】まず、鍵管理者装置100は、鍵管理者の指示にしたがい、乱数生成部101によって、乱数Sを生成し、これを鍵利用者の秘密鍵とする。その後、演算部102により秘密鍵Sを秘密情報S1、S2に分割し、秘密鍵S、および秘密情報S1、S2をメモリ106に格納する。次に、鍵管理者装置100は、メモリ106から秘密情報S1を取り出し、これを鍵管理者装置100に接続された計算機能付き記憶媒体300内のメモリ303に格納する。

【0023】鍵管理者は、秘密情報S1が格納された計算機能付き記憶媒体300を対象となる鍵利用者装置200に配布する。

【0024】秘密情報S1が格納された計算機能付き記憶媒体300を受け取った鍵利用者は、これを鍵利用者装置200に接続する。

【0025】鍵利用者装置200は、鍵利用者の指示にしたがい、計算機能付き記憶媒体300から秘密情報S1を取り出し、秘密情報S1と鍵管理者により予め付された当該鍵利用者の識別情報IDとを使って、鍵管理

者装置 100 との間で認証処理を行う。

【0026】認証処理には様々な方法があるが、ここでは、一例として、RSA 署名法を用いた場合とエルガマル署名法を用いた場合とについて、説明する。

【0027】まず、RSA 署名法を用いた場合について説明する。

* 【0028】鍵利用者装置 200 は、鍵利用者の指示にしたがい、予め以下の情報を、乱数生成部 201、素数生成部 202 および演算部 203 を用いて作成し、メモリ 205 に格納しておく。
【0029】
* 【数 1】

数 1

・ 秘密情報 p, q : 素数
・ 署名鍵 $(d, n), d \in \mathbb{Z}, n = pq$
・ 検証鍵 $(e, n), e \in \mathbb{Z}, n = pq \quad \dots(\text{数} 1)$

【0030】ここで、署名鍵は秘密、検証鍵は公開とする。鍵利用者装置 200 は、署名鍵と、鍵利用者が入力した、鍵管理者により予め付与された当該鍵利用者の識別情報 ID とを計算機能付き記憶媒体 300 に出力する。これを受けて、計算機能付き記憶媒体 300 は、演算部 302 により、

【0031】

【数 2】

数 2

$$AS = S^d \pmod{n} \quad \dots(\text{数} 2)$$

【0032】から認証情報 AS を計算する。ここで、S は、秘密情報 S1 と識別情報 ID とを入力とする所定の関数の値（たとえば、ハッシュ値）である。次に、計算機能付き記憶媒体 300 は、認証情報 AS を鍵利用者装置 200 に出力する。これを受けて、鍵利用者装置 200 は、通信部 206 により、認証情報 AS を、通信回線 400 を介して、鍵管理者装置 100 に送信する。

【0033】鍵管理者装置 100 は、通信部 107 により認証情報 AS を受信すると、認証部 104 により、

【0034】

【数 3】

数 3

$$S' = AS^e \pmod{n} \quad \dots(\text{数} 3)$$

【0035】が成立するか否かを検証し、成立すれば、認証情報 AS を送ってきた鍵利用者装置 200 の鍵利用者が正当な鍵利用者であると認証する。なお、鍵管理者装置 100 は、鍵利用者により付与した識別情報 ID を、当該鍵利用者によりオフラインで配布した計算機能付き記憶媒体 300 に格納された秘密情報 S1 と対応付けて、メモリ 108 に格納しているものとする。

【0036】次に、エルガマル署名法を用いた場合について説明する。

【0037】鍵利用者装置 200 は、鍵利用者の指示にしたがい、素数生成部 202 により素数 p を生成し、演

算部 202 により、

【0038】

【数 4】

数 4

$$\text{ord}_p(\alpha) = p-1 \quad \dots(\text{数} 4)$$

【0039】を満たす α を作成する。そして、作成した α および素数 p を計算機能付き記憶媒体 300 に出力する。これを受けて、計算機能付き記憶媒体 300 は、演算部 302 により、

【0040】

【数 5】

数 5

$$y = \alpha^s \pmod{p} \quad \dots(\text{数} 5)$$

【0041】を満たす y を計算し、署名鍵を (x, α , p)、検証鍵を (y, α , p) とする。ここで、S は、秘密情報 S1 と識別情報 ID とを入力とする所定の関数の値（たとえば、ハッシュ値）である。

【0042】次に、鍵利用者装置 200 は、p-1 と互いに素な乱数 k を乱数生成部 201 により作成し、

【0043】

【数 6】

数 6

$$r = a^k \pmod{p} \quad \dots(\text{数} 6)$$

【0044】を満たす r を計算する。さらに、適当なメッセージ m を乱数生成部 201 により生成し、r、k とともに計算機能付き記憶媒体 300 に出力する。これを受けて、計算機能付き記憶媒体 300 は、演算部 302 により、

【0045】

【数 7】

11
数7

12

$$t = (m - S')k^{-1} \pmod{p-1} \quad \dots(\text{数7})$$

【0046】を満たす t を計算する。そして、 (r, t) をメッセージ m に対する署名とし、メッセージ m 、署名 (r, s) を、鍵利用者装置200に出力する。これを受けて、鍵利用者装置200は、通信部206より、メッセージ m 、署名 (r, s) を、通信回線400を介して、鍵管理者装置100に送信する。

【0047】鍵管理者装置100は、メッセージ m 、署名 (r, s) を受け取ると、認証部104により、

【0048】

【数8】
数8

$$\alpha^m = y^r r^t \pmod{p} \quad \dots(\text{数8})$$

【0049】が成立するか否かを検証し、成立すれば、メッセージ m 、署名 (r, s) を送ってきた鍵利用者装置200の鍵利用者が正当な鍵利用者であると認証する。なお、鍵管理者装置100は、鍵利用者に付与した識別情報IDを、当該鍵利用者によってオフラインで配布した計算機能付き記憶媒体300に格納された秘密情報S1と対応付けて、メモリ106に格納しているものとする。

【0050】以上説明した認証処理により、鍵利用者が認証されると、鍵管理者装置100は、暗号化部103により、秘密情報S1を鍵として秘密情報S2を暗号化する。そして、通信部107により、暗号化された秘密情報S2を、通信回線400を介して、鍵利用者装置200に送信する。

【0051】鍵利用者装置200は、暗号化された秘密情報S2を受け取ると、これを計算機能付き記憶媒体300に出力する。これを受けて、計算機能付き記憶媒体300は、暗号化部301により、暗号化された秘密情報S2を、秘密情報S1を鍵として復号化し、メモリ303に格納する。さらに、演算装置302により、復号化された秘密情報S2、および秘密情報S1を基に、秘密鍵Sを復元し、メモリ303に格納する。

【0052】次に、鍵利用者装置200は、鍵利用者の指示にしたがって、計算機能付き記憶媒体300から秘密鍵Sを取り出し、この秘密鍵Sを使って、鍵管理者装置100との間で、上記と同様の手順により認証処理を行う。

【0053】なお、RSA署名法を用いる場合は、上記の(数2)、(数3)において、 S' の代わりに秘密鍵Sを用いばよい。また、エルガマル署名法を用いる場合には、上記の(数5)、(数7)において、 S' の代わりに秘密鍵Sを用いばよい。

【0054】鍵利用者が認証されると、鍵管理者装置100は、課金部105により、当該鍵利用者の、秘密鍵Sを用いた暗号通信に対する登録料金情報(課金情報)を生成し、これをメモリ106に格納する。この情報は、当該鍵利用者への料金請求に際して利用される。

10 【0055】上記の処理により、鍵利用者に秘密鍵Sが配布されると、鍵利用者は、秘密鍵Sを用いて、情報提供者との間で暗号通信を行う。あるいは、秘密鍵Sを用いて情報提供者との間で鍵共有を行った後に、その共有鍵により暗号通信を行う。

【0056】ここで、鍵管理者と情報提供者とが同一である場合における、鍵利用者および情報提供者間で暗号通信を行うためのシステムを図5に示す。図示するように、情報提供者装置500は、鍵管理者装置100により鍵利用者配布した秘密鍵Sを用いて、当該鍵利用者の鍵利用者装置200との間で、暗号通信を行う。

【0057】本実施形態では、鍵管理者は、秘密鍵Sを秘密情報S1、S2に分割し、秘密情報S1を記憶媒体(ICカード等の計算機能付き記憶媒体を含む)に搭載してオフラインで鍵利用者配布している。そして、秘密情報S2については、秘密情報S1および鍵利用者配布された識別情報IDを基に作成した認証情報ASにより鍵利用者を認証した場合にのみ、当該鍵利用者によってオンラインで送信するようにしている。

30 【0058】このようにすることで、たとえば、オフラインで配布した記憶媒体が不正者に盗用されたとしても、それだけでは、不正者は、秘密鍵Sを復元するのに必要なすべての秘密情報S1、S2を取得することができない。このため、秘密鍵情報を配布する際に、当該秘密鍵情報が不正者に横取りされる可能性を減少させることができ、ひいては、暗号通信のセキュリティを向上させることができる。

40 【0059】また、本実施形態において、鍵管理者装置100は、秘密情報S1および鍵利用者配布された識別情報IDを基に作成した認証情報ASにより鍵利用者が認証された場合、鍵利用者装置200に、秘密情報S2を、秘密情報S1を鍵として暗号化して送信し、鍵利用者装置200は、暗号化された秘密情報S2を、秘密情報S1を鍵として復号化し、復号結果と秘密情報S1とを基に、秘密鍵Sを復元している。このようにすることで、秘密情報S2をオンラインで送信する際のセキュリティをさらに向上させることができる。

50 【0060】なお、上記の実施形態では、秘密鍵Sを2つの秘密情報S1、S2に分割する場合について説明した。しかしながら、本発明はこれに限定されるものではなく、秘密鍵Sを少なくとも2つの秘密情報S1～Sn

に分割するようにしてもよい。この場合、そのうちの少なくとも1つをオフラインで配布し、残りを通信回線を使って、オンラインで送信するようにすればよい。

【0061】また、上記の実施形態では、鍵管理者装置100の課金部105により、課金情報を鍵管理者装置100内のメモリ106に格納するようにしたものについて説明したが、本発明はこれに限定されない。たとえば、課金部105を、鍵管理者装置100に設ける代わりに、鍵利用者装置200あるいは計算機能付き記憶媒体300に設け、課金情報を鍵利用者装置200内のメモリ205あるいは計算機能付き記憶媒体300内のメモリ303に格納するようにしてもよい。この情報は、鍵利用者への料金請求に際し、鍵管理者装置100に吸い上げられて利用される。

【0062】

【発明の効果】以上説明したように、本発明によれば、鍵管理者が鍵利用者に秘密鍵情報を配布する際、当該秘密鍵情報が不正者に横取りされる可能性を減少させることができ、ひいては、暗号通信のセキュリティを向上させることができる。

【図面の簡単な説明】

【図1】本発明の一実施形態である秘密鍵配布方法が適用されたシステムの概略図である。

* 【図2】図1に示す鍵管理者装置100の略機能構成図である。

【図3】図1に示す鍵利用者装置200の略機能構成図である。

【図4】図1に示す計算機能付き記憶媒体300の略機能構成図である。

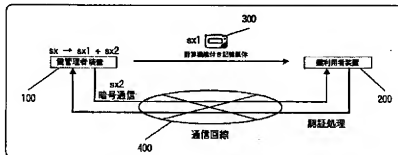
【図5】鍵管理者と情報提供者とが同一である場合における、鍵利用者および情報提供者間で暗号通信を行うためのシステムの概略図である。

10 【符号の説明】

- 100 鍵管理者装置
- 101、201 乱数生成部
- 102、203、302 演算部
- 103、204、301 暗号化部
- 104 認証部
- 105 課金部
- 106、205、303 メモリ
- 107、206 通信部
- 200 鍵利用者装置
- 202 素数生成部
- 300 計算機能付き記憶媒体
- 400 通信回線
- * 500 情報提供者装置

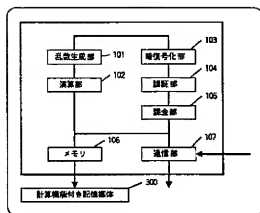
【図1】

図1



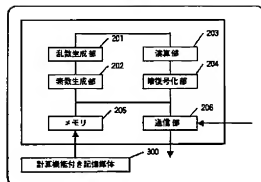
【図2】

図2



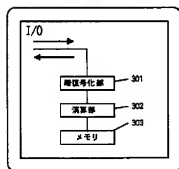
【図3】

図3



【図4】

図4



【図5】

図5

